UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 791 DEERFIELD BLVD, CINCINNATI OHIO 45245 DESCRIBED IN ATTACHMENT A-1 [INCLUDING ALL OUTBUILDINGS AND CURTILAGE]	)	Case No. **1:22-MJ-00628**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A-1

located in the SOUTHERN District of OHIO, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2) 18 U.S.C. 2252A(a)(5)(B)	distribution or receipt of child pornography; and possession of child pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jonathan P R Jones, FBI

Printed name and title

Sworn to before me and signed in my presence.
via electronic means, specifically Facetime video.

Date: **Nov 15, 2022**

Judge's signature

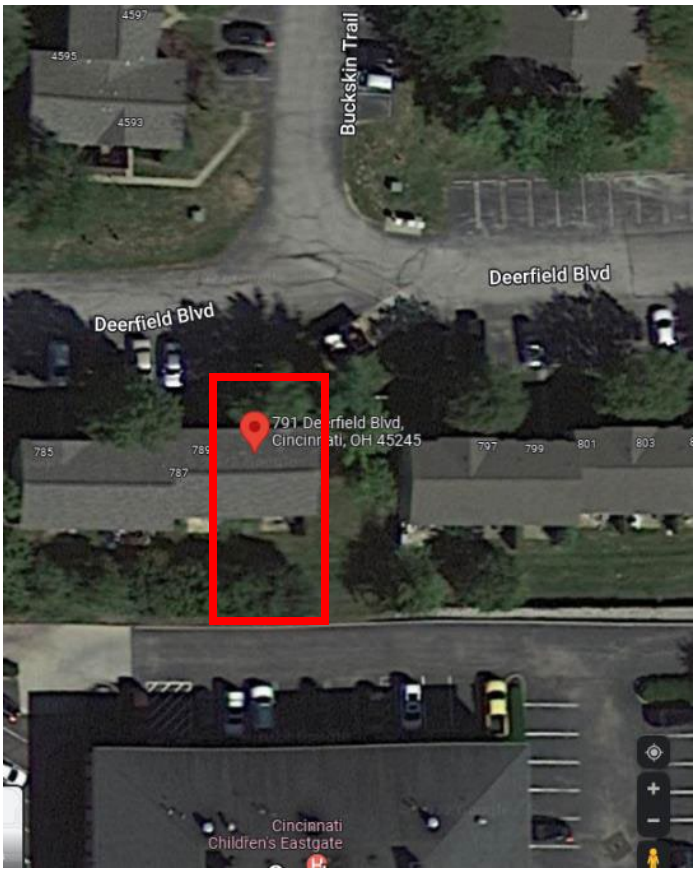
City and state: CINCINNATI, OHIO

Stephanie K. Bowman, United States Magistrate Judge

Printed name and title

ATTACHMENT A-1

The target address is 791 DEERFIELD BLVD, CINCINNATI OHIO 45245, which is located at southern side of the intersection of Deerfield Boulevard and Buckskin Trail in Union Township, Ohio. The residence is a two-story unit in a multi-unit building and is the eastern most unit in the building. The building is cream colored with blue shutters. The target address has a blue colored door with the numbers "791" affixed to the building to the right of the door. Any vehicle and/or exterior structure on the curtilage of the residence is included in the application for the search warrant associated with the residence. (See photographs below)


4597
4595
4593
Buckskin Trail
Deerfield Blvd
Deerfield Blvd
791 Deerfield Blvd,
Cincinnati, OH 45245
785
787
797
799
801
803
Cincinnati
Children's Eastgate

ATTACHMENT B-1

Particular Things to be Seized

1. Computer(s), cellphone(s), tablet(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, Kik and Telegram software and applications.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.

4. In any format or medium, all child pornography or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, or visual depictions.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography or any visual depictions.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child

pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concerns user attribution information.

13. Any and all cameras, film, videotapes, or other photographic equipment.

14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation.

15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.

16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.

18. Any records, bills, or other documents associated with internet service providers and telephone services.

19. Any records or communications in which sexually explicit material is being sent or received.

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
CINCINNATI, OHIO

IN THE MATTER OF THE SEARCH OF 791 DEERFIELD BLVD, CINCINNATI OHIO 45245 DESCRIBED IN ATTACHMENT A-1	**Case No.** 1:22-MJ-00628 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jonathan P R Jones, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation. I entered on duty as a special agent in 2007 and am currently assigned to the violent crime squad of the Cincinnati Division. In this capacity, I investigate matters involving crimes against children, human trafficking, criminal enterprises, and other violent crimes. Prior to Cincinnati, I was assigned to the Toledo Resident Agency and the Lima Resident Agency of the Cleveland Division, where I was assigned a wide array of criminal and national security matters. During my tenure as a law enforcement officer, I have investigated a range of state and federal criminal violations, including those involving white-collar crime, violent crime, drug trafficking, crimes against children matters, and national security investigations. Since 2006, I have received training and have experience in interviewing and interrogation techniques, arrest procedures, search and seizure, search warrant applications, and various other crimes and investigation techniques, to include several Title III investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Along with other agents and task force officers of the Federal Bureau of Investigation, I am currently involved in a child pornography investigation. This Affidavit is submitted in support of an application for a search warrant for the following:

   a. The residence located at 791 DEERFIELD BLVD, CINCINNATI OHIO 45245, which is a multi-story residence more fully described in Attachment A-1.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A(a)(2) - distribution or receipt of child pornography, and 18 U.S.C. § 2252A(a)(5)(B) - possession of child pornography, hereinafter the "subject offenses," have been committed by KEVIN BLAKE MERSHON and other unknown persons. There is also probable cause to

search the information described in Attachment A-1 for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B-1.

PERTINENT FEDERAL CRIMINAL STATUTES

5. This investigation concerns alleged violations of 18 U.S.C. § 2252A(a)(2) relating to the distribution or receipt of child pornography and 18 U.S.C. § 2252A(a)(5)(B) relating to the possession of child pornography.

a. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute– (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachments to this Affidavit:

a. **"Child Pornography"** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. **"Visual depictions"** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. **"Minor"** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. **"Sexually explicit conduct"** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite

sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

e. **"Internet Service Providers"** or **"ISPs"** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

f. A network **"server",** also referred to as a **"host"**, is a computer system that has been designated to run a specific server application or applications and provide requested services to a "client" computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.

g. **"Domain Name"** refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically ".com" for commercial organizations, ".gov" for the governmental organizations, ".org" for organizations, and, ".edu" for educational organizations. Second level names will further identify the organization, for example "usdoj.gov" further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as "www.usdoj.gov," to its currently assigned IP address (i.e., 149.101.1.32), to enable the flow of traffic across the Internet.

h. An "**Internet Protocol address"**, also referred to as an "**IP address"**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and

dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is connected to the Internet (or other network).

i. **"Log Files"** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

j. **"Hyperlink"** (often referred to simply as a **"link"**) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

k. **"Website"** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

l. **"URL"** or **"Uniform Resource Locator"** or **"Universal Resource Locator"** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

m. The terms **"records"**, **"documents"**, and **"materials"**, as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT, RECEIVE OR DISTRIBUTE CHILD PORNOGRAPHY

7. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

a. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings, or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings, or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain photos, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals with intent to view and/or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access online forums, such as bulletin boards, newsgroups, Internet relay chat or chat rooms are considered more advanced users and therefore more experienced in acquiring and storing a collection of child pornography images.

g. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

9. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 64 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer. Additionally, almost all cell phones today can record high-resolution photographs and videos.

10. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

11. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera or a cell phone, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person.

12. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

13. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

14. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

BACKGROUND REGARDING SEIZURE OF COMPUTERS

15. As stated, the investigation has determined that one or more computers (to include cellphones) have been used as an instrumentality in the course of, and in furtherance of, the offenses described above. Moreover, it is reasonable to believe that records and evidence are being stored in electronic form. This includes computer hard-drives, disks, CDs, modern cellphones and other similar electronic storage devices.

16. As indicated above, computer hardware is used to save copies of files and communications, while printers are used to make paper copies of same. Programs loaded on the drives are the means by which the computer can send, print and save those files and communications. Finally, password and security devices are often used to restrict access to or hide computer software, documentation, or data. Each of these parts of the computer is thus integrated into the entire operation of a computer. In order to best evaluate the evidence, the computers—and all of the related computer equipment described above—should be available to a computer investigator/analyst.

Forensic Imaging

17. An important step that is ordinarily part of an expert's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.

18. Special software, methodology, and equipment are used to obtain forensic images. Among other things, forensic images normally are "hashed," that is, subjected to a mathematical algorithm to the granularity of 10^{38} power, which is an incredibly large number that is much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity.

Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

Forensic Analysis

19. After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment, and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed, and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage, and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

20. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment, and software, also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. The computer may have stored information about the data at issue: who created it; when it was created; when it was last accessed; when it was last modified; when was it last printed; and when it was deleted. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence.

21. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search for information in text format. Many common electronic mail, database, and spreadsheet applications do not store data as searchable text. The contents of Adobe ".pdf" files are not searchable via keyword searches. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used email program that stores data in a non-textual, proprietary manner–ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners, yet they are not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text.

22. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be of limited probative value.

23. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques, and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained. Evidence in graphic file format must be laboriously reviewed by examiners. Criminals can mislabel and hide files and

directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files, and take other steps to defeat law enforcement.

Persistence of Digital Evidence

24. Computers store data, both on removable media (for example, CDs and floppy diskettes) and internal media, in ways that are not completely known or controlled by most users. Once stored, data is usually not destroyed until it is overwritten. For example, data that is "deleted" by a user is usually not actually deleted until it is overwritten by machine processes (rather than user decision) that decide where to store data and when overwriting will occur. Therefore, files and fragments of files and other data may easily last months, if not years, if the storage media is retained.

25. Typically, computer forensics focuses on at least three categories of data. These are: 1) **active data** – such as current files on the computer, still visible in file directories and available to the software applications loaded on the computer; 2) **latent data** – such as deleted files and other data that resides on a computer's hard drive and other electronic media in areas available for data storage, but which are usually inaccessible without the use of specialized forensic tools and techniques; and 3) **archival data** – such as data which has been transferred or backed up to other media such as CDs, floppy disks, tapes, and ZIP disks.

26. **Active data** includes not only files created by and with the user's knowledge, but also may include items such as Internet history log files, system registry files (listing all the systems and software applications installed on a computer, including the dates of installation, use, and deletion), and date/time file stamps automatically created that identify when files were created, modified, and last accessed.

27. **Latent data** includes data retained and stored on computer media in "unallocated" and "slack" space. Unallocated space refers to space on a hard drive that is available for the storage of new data. Slack space refers to any leftover space that remains when an active file is stored in particular location on the hard drive that is akin to an empty shelf in a closet containing other full shelves. Deleted files and other latent data that has not been overwritten by new data or files often may be accessed by a qualified forensic examiner from the unallocated and slack space on a computer user's hard drive months and years after such data was created by the user or the computer's operating system.

28. I know, based upon my training and experience, that a qualified forensic examiner may use knowledge of the mechanisms used to store electronic data to unlock and to uncover the activities of a computer's user years after the fact by examination of active, latent, and archival data. Through the use of proper computer forensic techniques such data and evidence of criminal offenses may be recovered, notwithstanding the passage of time since a crime occurred.

Conclusion Regarding Forensic Analysis Procedures

29. In light of these difficulties, I request permission for investigators to remove to a forensically-secure location the computers and computer-related equipment as instrumentality(ies) of the crimes, and to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant. Such action will greatly diminish the intrusion of law enforcement into the premises and will ensure that evidence can be searched for without the risk of losing, destroying, or missing the information/data for which there has been authorization to search.

30. Therefore, it is respectfully requested that the warrant sought by this application authorize the search and seizure for all "computer hardware," "computer software" and documents, which are more fully set-out and explained above, and further authorize a full physical and forensic examination of the seized items at a secure location.

PROBABLE CAUSE

31. In August 2019, investigators assigned to the FBI Cincinnati Child Exploitation/ Human Trafficking Task Force were contacted by the Milford (Ohio) Police Department (MPD) and the Lockland (Ohio) Police Department (LPD) concerning a joint investigation in which William J Bustillos III (DOB XX/XX/1993) and Joseph L Suder (DOB XX/XX/1983) were both arrested and charged, in Hamilton County and Clermont County respectively, for the sexual assaults of three minors, in addition to state level charges of production and distribution of child pornography. During a law enforcement interview admitted to producing sexually explicit images of the two male minors, in addition to an eight year-female. Suder admitted to sexually assaulting all three minors. Suder admitted to sending the sexually explicit images of the three minors to Bustillos. In return, Bustillos sent child pornography, of unknown minors, to Suder. Suder also admitted to trading images of the three minors in the Kik application group called “Cincinnati Taboo”. Unknown persons in the group sent Suder child pornography, of unknown victims, in exchange for providing images of the three minors. Suder told investigators he deleted the Kik application from his cell phone prior to the interview. During his law enforcement interview, Bustillos admitted to exchanging child pornography with Suder. Bustillos admitted to participating in the production of child pornography of the three minors. Bustillos admitted to sexually assaulting the five-year-old male victim on numerous occasions, while Suder assaulted the other two children at the same time. Bustillos advised he used Kik and another application to send and receive child pornography. Bustillos also participated in the Kik group called “CincyTaboo”. Bustillos advised he deleted the Kik application from his cell phone just prior to his interview.

32. In February 2020, investigators with the Hamilton County Sheriff’s Office – Regional Electronic Crimes Investigation unit (RECI) conducted an investigation based on an Ohio Internet Crimes Against Children Task Force lead. The investigation identified Ronald R Ledger Jr (DOB XX/XX/1977) as using the social media applications MeetMe and Kik to trade child pornography. During an interview, Ledger admitted to trading child pornography and to belonging to a Kik chat group called “Cincytabboo” in which child pornography was traded. Ledger provided investigators consent to search his cell phone and to assume control of his Kik account. RECI investigators captured the contents/communications from the Ledger’s Kik account. This included communications in the “Cincytabboo” chat group. The review identified “Cincytabboo” as being the group name, while the group hashtag was “#cincypervs”. Between approximately 02/26/2020 and 02/28/2020, RECI investigators monitored the communications in the “#cincypervs” chat group. On approximately 02/28/2020, the Ledger’s account was removed from the group by the group administrator. Investigators were unable to rejoin the group after that date. The group chat had approximately 43 members as of 02/26/2020. Approximately 18 of the account profiles included both a display name and a username, while the remaining profiles only provided a display name. A review of the captured “#cincypervs” group communications indicated the person with a display name “BASTILLA Shan” and username “BASTILLA_Shan” was an administrator in the group. The messages and images exchanged in the “#cincypervs” group included a message from username “BASTILLA_Shan”, which stated “Friendly reminder we have another group dedicated to young and only young stuff for those of u into it. Pm me. But will need new verification”

33. On 10/29/2020, Kik provided a search warrant return ((USDC-SDOH Case No: 1:21-MJ-362) for the "BASTILLA_Shan" account. The return contained 1,767 image and video files. A review of the files identified approximately 92 files which depicted prepubescent and post-pubescent males and females nude, partially nude, and/or engaged in sex acts, in which their genitals were depicted in lascivious manner which is consistent with child pornography as defined in 18 USC 2256.

34. The investigation identified the"BASTILLA_Shan" Kik account as being accessed from an IP address assigned to a residence at 5504 East Galbraith Road, Apartment 12, Cincinnati, Ohio 45236. In December 2020, employees with the apartment complex confirmed Jocko Rosello (Born XX/XX/1989) and his mother resided at the apartment. Criminal history checks indicated Rosello was arrested in 2016 and charged in Kentucky with a state violation of using an electronic communication system to procure a minor for sex. According to law enforcement reports, in July 2016 a law enforcement officer observed a Craigslist.com advertisement that was advertising "any girl into perv and taboo". The advertisement also advertised for a girl into incest, young, etc. An undercover law enforcement officer (UCO) responded to the advertisement under the guise of being a 14 year-old female. After exchanging emails, the UCO and Rosello switched to the Kik application. Rosello discussed wanting the UCO to send nude photographs and mentioned it would make him feel safer about coming to Louisville, Kentucky because he knew that law enforcement officers couldn't do that. Rosello also discussed viewing pornography, to include child pornography, with the UCO. Rosello also told the UCO he kept a collection of child pornography on a thumb drive.

35. In January 2021, FBI Cincinnati executed a residential search warrant (USDC-SDOH Case No: 1:21-MJ-029) at 5504 East Galbraith Road, Apartment 12, Cincinnati, Ohio 45236 The subject of the investigation, Jocko Rosello, was interviewed and several electronic devices were seized from the residence. Rosello was subsequently arrested and indicted in March 2021 on one count of Receipt and one count of possession of child pornography (18 USC § 2252A).

36. Upon review of the devices seized from Rosello's residence, more specifically an Alcatel One Touch Tablet, investigators determined that Rosello used social media applications to send and receive child pornography. A review of communications from the Kik application[1] identified February 2020 messages from Rosello's "iTheLilDevil" Kik account to a person with a Kik username of "Mershon_23" and a display name of "Kevin Mershon". In the message exchanges, Rosello sent an image of himself and several images and videos which depicted prepubescent males nude and/or engaged in sex acts. At the end of the Kik exchange, Rosello directed "Mershon_23" to use the Telegram application[2]. In the last message, "Mershon_23" sent a message with his apparent Telegram username of "mershow23".

---

[1] Kik Messenger, commonly called Kik, is a freeware instant messaging mobile app owned by holding company MediaLab.AI, Inc, and available free of charge on iOS and Android operating systems. It is a social networking application that permits a user to trade and disseminate various forms of digital media while using a cell phone or other digital device.

[2] Per open source information, Telegram is a freeware, cross-platform, cloud-based instant messaging, video calling, and voice calling service. It was initially launched in 2013. The app servers of Telegram are distributed worldwide to decrease data load, while operational center is currently based in Dubai. The application is available for Android, iOS, Windows, macOS and Linux, operating system. Telegram provides end-to-end encrypted calls and optional end-to-end encrypted "secret" chats between two online users on smartphone clients, whereas cloud chats use clientserver/server-client encryption. Users can send text and voice messages, animated stickers, make voice and videocalls, and share an unlimited number of images, documents, user locations, contacts, and music.

37. On or about 02/11/2020 several images/videos appeared to have been sent from Rosello's "iTheLilDevil" Kik account to the "Mershon_23" Kik Account. Examples of images/videos are described as follows:

a. An unnamed image of a nude prepubescent male is inserting his finger into his anus. The minor's face is not depicted, and the image only depicts his genitals, buttocks, and hand.
b. An unnamed image of a partially nude prepubescent male, less than 10 years old, in which the minor's face, chest, bare stomach, and erect penis are depicted. The image was taken from a angle in which the camera was closest to the minor's genitals.
c. An unnamed image of a nude prepubescent male, less than 10 years old, in which the part of the minor's face, chest, stomach, penis, and anus, are depicted. The image was taken from a angle in which the camera was closest to the minor's genitals.
d. A unamed image, which appeared to be a thumbnail image for a video, which depicted a small framed child grasping the erect penis of an adult male.[3]

38. A review of the Telegram application from the Alcatel tablet identified February 2020 communications between Rosello's Telegram account, username "ThatsYummy", telephone number "646-305-5985", and display name "Yum", and Telegram account with a username of "Mershow23", telephone number "513-501-7992", and display name of "Kevin S". In the exchange, Rosello and "Mershow23" remind each other that they originally met on the Grindr dating application and play the same video game. On 02/17/2020 "Mershow23" sent an image to Rosello, but the image was blurred in the forensic extraction report. On 02/19/2020, "Mershow23" sends a message "Okay" followed by "What's up". Rosello replied "Bout to cum a d sleep. U", then "and". "Mershow23" then stated "I would like to see some". Rosello then appeared to send several videos to "Mershow23". Due to the tablet being in airplane mode at the time of the forensic extraction, the videos, nor the associated thumbnail images, were loaded onto the device nor included in the forensic report. After the videos being sent, "Mershow23" replied "mhmm". Rosello messaged "Enjoy I gotta run sadly". "Mershow23" then messaged, "Aww", then, "Ok", then "I was also talking about seeing yours lol" The message exchange ended thereafter.

39. Pursuant to a December 2021 subpoena to Kik, the account with username of "Mershon_23" was created in September 2018 with an unconfirmed email address of dreammershon23@yahoo.com. Login IP information was provided from September 2018 to October 2021. A recurring IP address of 50.5.178.11 was identified as being used from 02/23/2021 to 10/25/2021.

40. Pursuant to a March 2022 subpoena to Cincinnati Bell, IP address 50.5.178.11 was identified as being assigned to the account of Kevin Mershon of 791 Deerfield Blvd, Cincinnati OH 45245-1235, telephone number 513-103-7369, from 3/10/2021 at 20:48 through 2/8/2022 at 19:33.

[3] A 23 second video, named "IMG_20200211_153415_851.mp4" was located in the forensic extraction of the above referenced Alcatel tablet. The video depicts a prepubescent female engaged in oral sex on an adult male. The thumbnail image from the Kik chat appears to match likeness of the minor, her clothing, and other details depicted in this video.

41. Pursuant to a February 2022 subpoena to TMobile, telephone number 513-501-7992 was identified as an active account being assigned to a Michelle R Scott of 791 Deerfield Boulevard, Cincinnati, OH 45245 USA since 03/12/2019.

42. In March 2022, an FBI Online Covert Employee located the "Mershon_23" Kik account. The profile image for the account depicted a white male wearing glasses.

43. Pursuant to a March 2022 subpoena to Kik, the account with username of "Mershon_23" was shown to have additional logins from an IP address of 72.49.6.10 from 02/12/2022 to 02/28/2022.

44. Pursuant to a March 2022 subpoena to Cincinnati Bell, IP address 72.49.6.10, was identified as being assigned to the account of Kevin Mershon of 791 Deerfield Blvd, Cincinnati OH 45245-1235, telephone number 513-103-7369, from 2/8/2022 at 21:05 through 4/1/2022 at 13:52.

45. Commercial and law enforcement database queries identified a Kevin Blake Mershon, Born XX/XX/1996, Social Security Account Number XX-XX-7247, as matching the likeness of the profile image from the "Mershon_23" Kik account. No criminal history was located for Mershon. A commercial database query identified telephone number 513-501-7992 as being associated with Mershon.

46. In April 2022, the Union Township Police Department advised the agency had two October 2021 reports involving menacing and domestic violence in which Mershon was identified as residing at 791 Deerfield Blvd, Cincinnati OH 45245. A commercial database provided a narrative of UTPD incidents. The reports identified Mershon and his mother, Michele Scott, both residing at 791 Deerfield Blvd, as filing complaints against Michele's husband.

47. On 08/31/2022, the leasing manager of the 860East apartment complex confirmed Mershon, Scott, and Scott's daughter, Brittany Scott, currently resided at 791 Deerfield Blvd, Cincinnati OH 45245 since December 2019. Another adult male, Jason Wolfe, identified as Michelle Scott's boyfriend, moved into the residence in October 2021. Mershon's telephone number was identified as 513-501-7992.

48. Intermittent surveillance, between 07/07/2022 and 11/02/2022, of 791 Deerfield Blvd, Cincinnati OH 45245 has not revealed significant activity at the residence. Vehicles registered to Jason Wolfe and a Freddie M Reedy were observed parked in front of the residence. Commercial database information indicates Mershon and Reedy shared a common residence in West Portsmouth, Ohio since 2013.

49. As of 11/02/2022 the "Mershon_23" Kik account was identified as being an active account for 1,514 days. As of the same date, the Telegram account with a username of "Mershow23" was not located, indicating it was not active.

CONCLUSION

50. Based on the evidence in this investigation, I believe KEVIN BLAKE MERSHON received, and possessed, and distributed child pornography at the residence 791 DEERFIELD BLVD, CINCINNATI OHIO 45245. Based on the foregoing, I request that the Court issue the proposed search warrants.

REQUEST FOR SEALING

51. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

	Respectfully submitted,  Jonathan P R Jones Special Agent Federal Bureau of Investigation

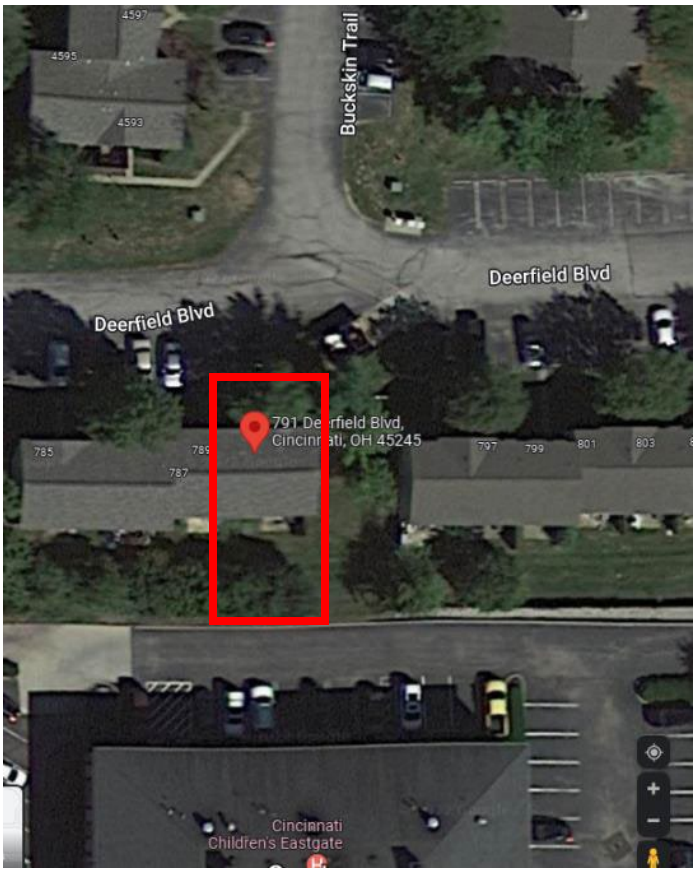
Subscribed and sworn to before me on this 15th day of November, 2022
via electronic means, specifically Facetime video.

Stephanie K. Bowman

THE HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF OHIO

ATTACHMENT A-1

The target address is 791 DEERFIELD BLVD, CINCINNATI OHIO 45245, which is located at southern side of the intersection of Deerfield Boulevard and Buckskin Trail in Union Township, Ohio. The residence is a two-story unit in a multi-unit building and is the eastern most unit in the building. The building is cream colored with blue shutters. The target address has a blue colored door with the numbers "791" affixed to the building to the right of the door. Any vehicle and/or exterior structure on the curtilage of the residence is included in the application for the search warrant associated with the residence. (See photographs below)


Buckskin Trail
Deerfield Blvd
Deerfield Blvd
Cincinnati
Children's Eastgate

ATTACHMENT B-1

Particular Things to be Seized

1. Computer(s), cellphone(s), tablet(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, Kik and Telegram software and applications.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.

4. In any format or medium, all child pornography or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, or visual depictions.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography or any visual depictions.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child

pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concerns user attribution information.

13. Any and all cameras, film, videotapes, or other photographic equipment.

14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation.

15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.

16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.

18. Any records, bills, or other documents associated with internet service providers and telephone services.

19. Any records or communications in which sexually explicit material is being sent or received.